PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-265432
(43)Date of publication of application : 28.09.1999

(51)Int.CI. G06K 19/10
E05B 49/00
G06K 17/00

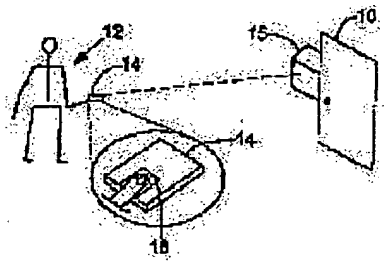
(21)Application number : 10-365679
(22)Date of filing : 22.12.1998

(71)Applicant : TRW INC
(72)Inventor : HSU SHI-PING
LING JAMES M
MESSENGER ARTHUR F
EVANS BRUCE W

(30)Priority
Priority number : 97 995267 Priority date : 22.12.1997 Priority country : US

(54) PERSONAL IDENTIFICATION FOB

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device for automatically verifying the identity of a person, who tries to access his properties to be protected such as an automobile, room, building or automatic teller machine, and a method for using the device.
SOLUTION: This device is disclosed in the form of a hand-held fob 14 and is provided with a sensor 16 for reading biometrological data such as fingerprints from a person 12 and a collation part for discriminating the detected data by comparing them with a previously stored reference image. In the case of matching, the fob 14 starts exchanging signals with a 'door' 10 for protecting his property. The fob 14 generates a numerical value like a cyclic redundant code from the stored reference image, enciphers this numerical value, defines it as identity of the person and transmits it to the door 10. In order to improve security, the person 12 registers this numerical value for each door 10 desired to be accessed. When the confirmation of identity is received from the fob 14, the door 10 compares before the permission of access the received numerical value with a numerical value stored during registration.



LEGAL STATUS

[Date of request for examination] 22.12.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－265432

(43)公開日　平成11年(1999)９月28日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｓ
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｒ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｖ

審査請求　有　　請求項の数21　ＯＬ　（全 12 頁）

(21)出願番号　特願平10－365679

(22)出願日　平成10年(1998)12月22日

(31)優先権主張番号　９９５２６７

(32)優先日　1997年12月22日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591169755
ティーアールダブリュー・インコーポレーテッド
ＴＲＷ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国オハイオ州44124，リンドハースト，リッチモンド・ロード　1900

(72)発明者　シーピン・スー
アメリカ合衆国カリフォルニア州91107，パサディナ，サウス・ポニータ・アベニュー　461

(74)代理人　弁理士　社本　一夫　（外５名）

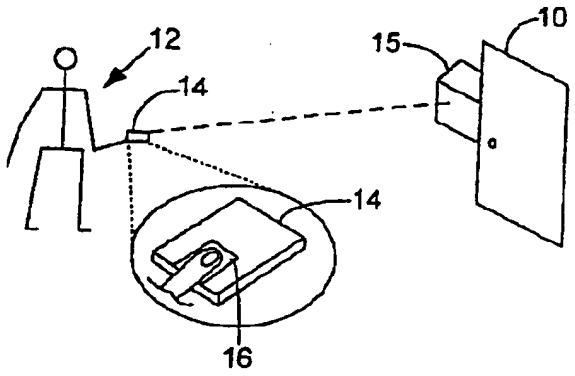
最終頁に続く

(54)【発明の名称】　個人識別フォブ

(57)【要約】

【課題】　自動車、部屋、建物または自動預金支払機等の保護対象所有物に対してアクセスしようとする人の同一性を自動的に検証する装置、およびその使用方法を提供する。

【解決手段】　この装置は、ハンドヘルド・フォブ（１４）の形態で開示され、指紋のような生物測定学的データを人（１２）から読み取るセンサ（１６）と、検知したデータを、予め格納してある基準画像（３２）と比較し、判定を行う照合部（２８）とを含む。一致があった場合、フォブ（１４）は、所有物を保護する「ドア」（１０）と信号の交換を開始する。フォブ（１４）は、格納してある基準画像（３２）から、巡回冗長符号のような数値を発生し、この数値を暗号化し、それを人の同一性の確認としてドア（１０）に送信する。安全性を高めるために、人（１２）は、アクセスを望むドア（１０）毎にこの数値を登録する。フォブ（１４）からの同一性確認の受信時に、ドア（１０）は、アクセスを許可する前に、受信した数値を、登録の間に格納した数値と比較する。



1

【特許請求の範囲】

【請求項１】　保護対象所有物に対してアクセスを求める人の同一性を自動的に検証する装置であって、
保護対象所有物に対してアクセスを求める人を識別する生物測定学的データを読み込むセンサと、
前記保護対象所有物に対してアクセスを有することを許可された人を識別する基準生物測定学的データを格納する記憶手段と、
前記格納されている基準生物測定学的データを、前記アクセスしようとする人の生物測定学的データと比較し、これらが一致するか否かについて判定を行う照合部と、
同一性確認をドアに安全に通信し、前記同一性確認の受信時に、前記保護対象所有物に対するアクセスを与える手段と、を備えた装置。

【請求項２】　請求項１記載の装置であって、更に、
検証モードにおいて前記装置の動作を開始する第１のスイッチと、前記装置を登録動作モードに置くように作動する第２のスイッチとを有するユーザ・インターフェースを備え、前記センサからの生物測定学的データを前記記憶手段に格納し、前記検証動作モードにおいて後に検索する、装置。

【請求項３】　請求項１記載の装置において、
前記センサ、前記記憶手段および前記照合部が全て、携帯機器に内蔵されている、装置。

【請求項４】　請求項３記載の装置において、
前記センサ、前記記憶手段および前記照合部が全て、前記人が携行する携帯フォブに内蔵されている、装置。

【請求項５】　請求項３記載の装置において、
前記センサ、前記記憶手段および前記照合部が全て、前記保護対象所有物から離れた通信機器に内蔵されている、装置。

【請求項６】　請求項３記載の装置において、前記安全に同一性確認を通信する手段が、
前記格納されている基準生物測定学的データから数値を発生する手段と、
前記数値を暗号化する暗号化ロジックと、
前記暗号化数値を、前記人に対する識別データと共に前記ドアに送る通信インターフェースと、を含み、前記送信された数値が、登録手続の間に前記人によって予め与えられたものと同じであることを確認した場合、前記ドアが前記保護対象所有物に対する所望のアクセスを与える、装置。

【請求項７】　請求項６記載の装置であって、更に、
前記ドアによって発生されかつ送信された暗号キーを受信する受信機と、
前記携帯機器内に秘密暗号キーを格納する手段と、
を備え、前記暗号化ロジックが、前記ドアから受信した前記暗号キーと前記秘密暗号キーとを用いて、前記数値に二重暗号化を施す、装置。

【請求項８】　個人識別フォブであって、保護対象所有物に対するアクセスのために当該フォブを用いようとするユーザの同一性を自動的に検証し、
保護対象所有物に対してアクセスしようとするユーザを識別する指紋データを読み取るセンサと、
登録手続の間に前記ユーザの基準指紋画像を格納し、今後の使用のために該基準画像を保持するメモリと、
前記格納されている基準画像を、前記アクセスしようとするユーザの前記センサから得られた指紋画像と比較し、２つの画像が一致するか否かについて判定を行う画像照合部と、
同一性確認をドアに安全に通信し、該同一性確認の受信時に、前記保護対象所有物に対するアクセスを与える手段と、を備えたフォブ。

【請求項９】　請求項８記載の個人識別フォブにおいて、前記同一性確認を安全に通信する手段が、
前記格納されている基準指紋画像から数値を発生する手段と、
前記数値を暗号化する暗号化ロジックと、
前記暗号化数値を、前記ユーザ識別データと共に前記ドアに送る送信機と、を含み、前記送信された数値が、登録手続の間に前記ユーザによって予め与えられたものと同じであることを確認した場合、前記ドアが前記保護対象所有物に対する前記所望のアクセスを与える、個人識別フォグ。

【請求項１０】　請求項９記載の個人識別フォブにおいて、
前記数値を発生する手段が、前記格納されている基準指紋画像から巡回冗長符号を発生する手段を含む、個人識別フォグ。

【請求項１１】　請求項９記載の個人識別フォグであって、更に、
前記ドアによって発生されかつ送信された暗号キーを受信する受信機と、
前記フォブ内に秘密暗号キーを格納する手段と、を備え、前記暗号化ロジックが、前記ドアから受信した前記暗号キーと、前記秘密暗号キーとを用いて、前記数値に二重暗号化を施す手段を含む、個人識別フォグ。

【請求項１２】　ドアによって保護されている所有物に対してアクセスしようとするユーザの同一性を自動的に検証する方法であって、
前記ユーザが携行する個人識別機器の一部であるセンサによって、ユーザの生物測定学的データを検知するステップと、
前記検知した生物測定学的データを、前記個人識別機器内に予め格納してある基準生物測定学的データと比較するステップと、
前記検出した生物測定学的データが前記基準生物測定学的データと一致するか否かについて判定を行うステップと、
一致があった場合、前記保護対象所有物に対するアクセ

スを制御するドアに、同一性確認を安全に伝達するステップと、
前記ドアにおいて前記ユーザの同一性を確認した場合、所望のアクセスを与える機器を作動させるステップと、を含む方法。
【請求項１３】　請求項１２記載の方法であって、更に、
手動スイッチによって、前記個人識別機器の通常動作を開始するステップを含む、方法。
【請求項１４】　請求項１２記載の方法であって、更に、
アクセスしようとするために前記ドアに近づいた場合、該ドアから「起動」メッセージを受信するステップと、
前記「起動」メッセージを受信した場合、前記個人識別装置の通常動作を開始するステップと、を含む、方法。
【請求項１５】　請求項１２記載の方法において、前記安全に通信するステップが、
前記格納されている基準生物測定学的データから数値を発生するステップと、
前記数値を暗号化するステップと、
前記暗号化数値を前記ドアに送信するステップと、
ユーザ識別データを前記ドアに送信するステップと、
前記ドアにおいて、前記暗号化数値を受信しかつ解読するステップと、
前記ドアにおいて登録プロセスの間に前記ユーザによって予め格納されている数値と、前記解読した数値とを比較し、前記ユーザの同一性を確認するステップと、
前記ユーザの同一性が確認された場合、所望の機能を活性化させ、前記保護対象所有物に対するアクセスを与えるステップと、を含む方法。
【請求項１６】　請求項１５記載の方法において、前記安全に通信するステップが、更に、
前記ドアにおいて、ドア公開暗号キーおよびドア秘密暗号キーのランダム対を発生するステップと、
前記ドア公開キーを前記個人識別機器に送信するステップと、
前記機器のそれ以降の使用全てのために、公開および秘密暗号キーの対を、前記個人識別機器に対して選択するステップと、
前記ドア登録プロセスの一部として、前記個人識別機器の公開キーを前記ドアに与えるステップと、
前記個人識別機器の秘密キーを前記機器内に機密的に格納するステップと、を含み、
前記暗号化ステップが、前記ドアの公開キーおよび前記個人識別機器の秘密キーを用いて、前記数値に二重暗号化を施すステップを含む、方法。
【請求項１７】　請求項１６記載の方法において、前記ドアが、
前記個人識別機器の公開キーおよび前記ドアの秘密キーを用いて、前記二重に暗号化された数値を解読する追加

のステップを実行する、方法。
【請求項１８】　正常に施錠されたドアによって保護されている所有物に対するアクセスをユーザが得るための方法であって、
ドアに近づきつつ、フォブ内の指紋センサ上に指を置くステップと、
前記フォブを作動させ、前記ユーザの指紋を検知させかつ記録させるステップと、
前記検知した指紋を、前記フォブ内に予め格納してある基準指紋データと比較するステップと、
比較において合格した場合、前記フォブから、前記所有物を保護する前記ドアに同一性確認を送信するステップと、
同一性確認の受信時に、前記ドアを開錠するステップと、を含む方法。
【請求項１９】　請求項１８記載の方法において、同一性確認を送信する前記ステップが、
前記フォブにおいて前記同一性確認を暗号化するステップと、
前記ドアにおいて前記同一性確認を解読するステップと、を含む、方法。
【請求項２０】　請求項１９記載の方法において、
前記暗号化ステップが、二重暗号化を施すステップを含み、
前記解読ステップが、二重に解読するステップを含む、方法。
【請求項２１】　請求項２０記載の方法において、
前記二重暗号化を施すステップが、最初に、前記ドア内において発生し、該ドアから受信した公開ドア暗号キーを用いて、前記同一性確認を暗号化し、次いで前記フォブ内に格納されている秘密フォブ暗号キーを用いて更に暗号化を行うステップを含み、
前記二重に解読するステップが、最初に、前記ドアにおける以前の登録時に前記ユーザによって与えられた公開フォブ暗号キーを用いて解読を行い、次いで前記ドアにおいて発生した秘密ドア暗号キーを用いて解読を行うステップを含む、方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、一般的に、個人識別または検証システムに関し、更に特定すれば、何らかの貴重品へのアクセスを許可する前に、人の同一性（ｉｄｅｎｔｉｔｙ）を自動的に検証するシステムに関するものである。
【０００２】
【従来の技術】従来より、所有物（ｐｒｏｐｅｒｔｙ）にアクセスする権利を有する人のみが必要な鍵またはダイヤル錠用コンビネーション（ｃｏｍｂｉｎａｔｉｏｎ）を有するという推測に基づいて、鍵および錠、または組み合わせ錠（ダイヤル錠）を用いて、当該所有物に

対するアクセスを制限している。勿論、この従来からの手法は、部屋、建物、自動車および銀行内の貸し金庫（safe deposit box）を含む種々の閉鎖空間に対するアクセスを制限するために、今でも広く用いられている。近年、機械的な錠は、例えば、ホテルの部屋のドア、または銀行の自動預金支払機（ATM：automatic teller machine）に対するアクセスに用いられるような、符号化プラスチック・カードによって作動する電子的な錠に取って代わられつつある。後者の場合、銀行口座の「キー」のようなプラスチック・カードのユーザは、アクセスが許可されるには、同様に個人識別番号（PIN）を供給しなければならない。

【0003】多くの自動車は、錠および侵入アラーム（intrusion alarm）双方によって保護されており、典型的に、自動車の所有者がキー・チェーン・フォブ（key chain fob）として携行する小さな無線または赤外線送信機を用いて、その活性化（作動）および不活性化（不作動）を行う。この種の機器は便利であるが、所有者がそれを紛失した場合に、機械式の鍵を安全の確保のために用いた場合と同様に、車両の弱点になる可能性がある。

【0004】今日では、人は自宅、仕事場および自動車に入るための種々の鍵、ならびに銀行口座や店の掛け売り勘定（charge account）のような金融資産にアクセスするためにプラスチック・カードの束も携行する必要があり、しかもその束は増々厚くなりつつある。今日の多忙な人は、いくつかのパスワードおよびPINを記憶しておき、プラスチック・カードと共に用いたり、同様にコンピュータ・ソフトウエアにアクセスする際に用いなければならない。コンピュータ・ソフトウエアの場合、アクセス・カードを必要とする場合もしない場合もある。更に、アクセスを制限するための前述の機器は全て、盗難、複製および悪用の危険性がある。機械的な鍵によって保護されている資産が最も危ないが、もちろん、コンビネーション、パスワードおよびPINによって保護されている資産にも、適切なコンビネーション、パスワードまたはPINを盗み出したり、推論したり、または想像した無許可のユーザによる違法の進入を受ける可能性がある。

【0005】

【発明が解決しようとする課題】したがって、個人の所有物およびその他の貴重な資産に対するアクセスを制限するための技法、およびその信頼性強化に対する必要性が、広く存在する。理想的には、この技法は、アクセスしようとする人の同一性を確実に検証し、多数の鍵やスキャナブル・カード（scannable card）を携行する必要性、およびコンビネーション、パスワードおよびPINを記憶する必要性をなくすべきである。本発明は、この要望を満たすものである。

【0006】

【課題を解決するための手段】本発明は、保護対象所有物にアクセスしようとする人の同一性を自動的に検証する装置およびその使用のための方法にある。保護対象所有物は、建物、部屋、自動車、金融口座のように、様々な形態を取り得る。説明の目的のために、保護対象所有物に対するアクセスは、「ドア」を通じて得られると言うことにする。多くの場合、所有物が例えば自動車、部屋または建物とすると、アクセスを得るための物理的なドアを実際に有する。他の形態の保護対象所有物には、物理的な入り口（entry door）を有さないが、本発明の目的のために「ドア」を有すると見なせるものもある。本発明の重要な態様によれば、人は、ユーザの直ぐ隣に位置するドアまたは数千マイルも離れたドアに、安全にアクセスすることができる。

【0007】端的にそして一般的なことばで述べると、本発明の装置は、保護対象所有物に対してアクセスしようとする人を識別する生物測定学的（biometric）データを読み込むセンサと、前述の保護対象所有物に対してアクセスを有することを許可された人を識別する基準生物測定学的データを格納する記憶手段と、格納されている基準生物測定学的データを、アクセスしようとする人の生物測定学的データと照合し、これらが一致するか否かについて判定を行う相関器（照合部）と、同一性確認をドアに安全に伝達し、同一性確認の受信時に、保護対象所有物に対するアクセスを与える手段とを備える。本装置は、更に、検証モードにおいて装置の動作を起動する第1のスイッチと、装置を登録動作モードに置くように作動する第2のスイッチとを有するユーザ・インターフェースを備えることができ、センサからの生物測定学的データを記憶手段に格納し、検証動作モードにおいて後に検索する。

【0008】以下に開示する本発明の実施形態では、センサ、記憶手段および照合部は全て、携帯機器に内蔵され、この携帯機器は、人が携行するフォブ、保護対象所有物から離れた何らかのその他の形態の通信機器とすることができる。開示する実施形態では、安全に同一性確認を通信する手段は、格納されている基準生物測定学的データから数値を発生する手段と、数値を暗号化する暗号化ロジックと、暗号化した数値を人に対する識別データと共にドアに送る通信インターフェースとを含む。送信された数値が、登録手続の間に人によって予め与えられたものと同じであることを確認した場合、ドアが保護対象所有物に対する所望のアクセスを与える。

【0009】更に、本発明の装置は、ドアによって発生されかつ送信された暗号キーを受信する受信機と、携帯機器内に秘密暗号キーを格納する手段とを含むことができる。更に、機器内の暗号化ロジックは、ドアから受信した暗号キーと秘密暗号キーとを用いて、数値に二重暗号化を施す手段を含む。

【0010】本発明の装置は、携帯フォブとして定義することもでき、この場合、携帯フォブは、保護対象所有物に対してアクセスしようとするユーザを識別する指紋データを読み取るセンサと、登録手続の間にユーザの基準指紋画像を格納し、今後の使用のために該基準画像を保持するメモリと、格納されている基準画像を、アクセスしようとするユーザのセンサから得られた指紋画像と比較し、2つの画像が一致するか否かについて判定を行う画像照合部（イメージ相関器）と、同一性確認をドアに安全に伝達し、該同一性確認の受信時に、保護対象所有物に対するアクセスを与える手段とを含む。更に特定すると、同一性確認を安全に伝達する手段は、格納されている基準指紋画像から数値を発生する手段と、数値を暗号化する暗号化ロジックと、暗号化した数値を、ユーザ識別データと共にドアに送る送信機とを含む。送信された数値が、登録手続の間にユーザによって予め与えられたものと同じであることを確認した場合、ドアが保護対象所有物に対する所望のアクセスを与える。

【0011】前の段落で定義した個人識別フォブにおいて、数値を発生する手段は、格納されている基準指紋画像から巡回冗長符号を発生する手段を含む。更に、フォブは、ドアによって発生されかつ送信された暗号キーを受信する受信機と、フォブ内に秘密暗号キーを格納する手段とを含む。フォブ内の暗号化ロジックは、ドアから受信した暗号キーと、秘密（プライベート）暗号キーとを用いて、数値に二重暗号化を施す手段を含む。

【0012】新規な方法として、本発明は、ユーザが携行する個人識別機器の一部であるセンサによって、ユーザの生物測定学的データを検知するステップと、検知した生物測定学的データを、個人識別機器内に予め格納してある基準生物測定学的データと比較するステップと、検出した生物測定学的データが基準生物測定学的データと一致するか否かについて判定を行うステップと、一致があった場合、保護対象所有物に対するアクセスを制御するドアに、同一性確認を安全に伝達するステップと、ドアにおいてユーザの同一性を確認した場合、所望のアクセスを与える機器を作動させるステップとから成る。本方法は、更に、手動スイッチによって、個人識別機器の通常動作を開始するステップも含む。

【0013】一実施形態において、本方法は、アクセスしようとするためにドアに近づいた場合、該ドアから「起動（ｗａｋｅ－ｕｐ）」メッセージを受信するステップと、「起動」メッセージを受信した場合、個人識別装置の通常動作を開始するステップとを任意に含む。安全に通信するステップは、格納されている生物測定学的データから数値を発生するステップと、数値を暗号化するステップと、暗号化した数値をドアに送信するステップと、ユーザ識別データをドアに送信するステップと、ドアにおいて、暗号化した数値を受信しかつ解読するステップと、ドアにおいて登録プロセスの間にユーザによって予め格納されている数値と、解読した数値とを比較し、ユーザの同一性を確認するステップと、ユーザの同一性が確認された場合、所望の機能を活性化させ、保護対象所有物に対するアクセスを与えるステップとを含む。

【0014】更に特定すれば、安全に通信するステップは、更に、ドアにおいて、ドア公開暗号キーとドア秘密暗号キーとのランダム対を発生するステップと、ドア公開キーを個人識別機器に送信するステップと、機器のそれ以降の使用全てのために、公開暗号キーと秘密暗号キーとの対を、個人識別機器に選択するステップと、ドア登録プロセスの一部として、個人識別機器の公開キーをドアに与えるステップと、個人識別機器の秘密キーを機器内に機密的に格納するステップとを含む。暗号化ステップは、ドアの公開キーおよび個人識別機器の秘密キーを用いて、数値に二重暗号化を施すステップを含む。本方法は、更に、個人識別機器の公開キーおよびドアの秘密キーを用いて、二重に暗号化された数値を解読するステップを含み、これをドアにおいて実行する。

【0015】以上の説明から、本発明は、建物、自動車、コンピュータ、または他のあらゆる保護対象所有物に対して安全なアクセスを与えるという点において、飛躍的な進歩を表すことが認められよう。即ち、本発明は、単一のセキュリティ機器を用いて、多数の所有物または資産へのアクセスを可能とする。このセキュリティ機器は、指紋のような生物測定学的なデータを用いて、その所有者を容易に識別する。識別は小型の携帯機器内で検証されるので、保護対象所有物への多数の「ドア」との通信は単純な同一性確認メッセージに限定し、これには適切な暗号化を施すことによって、盗聴またはリバース・エンジニアリングを防止することができる。本発明のその他の態様および利点は、添付図面と関連付けた、以下の更に詳細な説明から明らかとなろう。

【0016】

【発明の実施の形態】例示の目的で図面に示すように、本発明は、保護対象所有物にアクセスしようとする人の同一性を自動的に検証するシステムに関するものである。従来、所有物は、機械的な錠および鍵、あるいはコンビネーション、パスワードおよび個人識別番号（ＰＩＮ）の記憶を必要とする、組み合わせ錠や電子機器の組み合わせによって保護されてきた。

【0017】本発明によれば、保護対象所有物にアクセスしようとする人は、その人に関連する、選択した生物測定学的測定値を得ることができるセンサを含む携帯機器を携行し、保護対象所有物の「ドア」付近に位置し、関係付けられた機器と通信する。好ましくは、携帯機器は、同一性検証手段も含む。センサから得た生物測定学的測定値を、予め行われた登録手続の間に同じ人から得た1組の基準生物学的測定値に含まれる、対応する測定値と比較する。

【００１８】図１は、保護対象所有物への「ドア」を開くために本発明をいかにして用いるかを概略的に示す。ドアを参照番号１０で示す。ドア１０に入ろうとする人１２は、小型ハンドヘルド機器１４を携行する。このハンドヘルド機器１４は、フォブ（ｆｏｂ）の形状を取ることができる。フォブ１４は、ドア１０付近に配置された受信機１５と通信する。この好適な実施形態では、フォブ１４または同様の携帯機器は、生物測定学的センサを含み、この好適な実施形態では指紋センサ１６である。しかしながら、本発明の原理は、解剖学的構造の他の部分からの印刷パターン、または目の虹彩パターンのように、ユーザ１２を識別する他の生物測定学的特性を採用する装置にも適用可能であることは理解されよう。

【００１９】ユーザ１２がセンサ１６上に指を置き、スイッチを作動させると、その人の指紋が走査され、フォブ１４内に格納してある基準指紋画像と比較される。フォブ１４は、この目的のために、指紋照合部（相関器）を含む。比較の結果、一致が得られた場合、フォブ１４は確認メッセージをドア１０に送信し、ドア１０が開いてユーザ１２によるアクセスが許可される。

【００２０】ドア１０に送られる確認メッセージの性質は非常に重要である。何故なら、標準的なフォーマットの単純な「ＯＫ」または「開放」メッセージ信号では、「クローン（ｃｌｏｎｉｎｇ）」プロセスにおいて容易に複製が作られ、無許可のアクセスは比較的単純に行われてしまうからである。理想的には、確認メッセージは、異なるアクセス「ドア」に対して同じフォーマットであるが、その複製を防止し、かつフォブ１４のリバース・エンジニアリングを防止するような方法で符号化または暗号化したものでなければならない。これらの目標を達成するための一技術の詳細について、以下で説明する。

【００２１】図２は、フォブ１４の主要構成部品を示し、それには指紋センサ１６、プロセッサ・モジュール２０、トランシーバ（送受信機）２２およびバッテリ電源２４が含まれる。指紋センサ１６は、入手可能な設計のものであればいずれでもよく、容量式センサまたは光学式センサを含むことができる。センサ１６は、ユーザの指紋の一部分の２進またはグレースケール・イメージ（画像）を生成する。迅速な処理のためには、続く比較プロセスでは、画像全体を用いない方がよく、代わりにセンサ１６が供給するのは、指紋の嶺および谷の全てを含む、指紋の詳細な「マップ」である。プロセッサ・モジュール２０を、図３に詳細に示す。

【００２２】プロセッサ・モジュール２０は、プロセッサ２６を含み、これは、例えば、ＲＩＳＣ（縮小命令セット・コンピュータ）プロセッサ、本発明の好適な実施形態における特徴照合部（ｃｏｒｒｅｌａｔｏｒ）２８である指紋一致検出部、巡回冗長符号（ＣＲＣ）発生部３０、基準指紋画像用記憶部３２、暗号化ロジック３４

および秘密（プライベート）暗号キー用記憶部３６を含むことができる。また、フォブ１４は、ユーザ・インターフェース３８も含み、ユーザ１２はこれを通じて種々のモードの動作を起動する。基本的に、ユーザ・インターフェース３８は、指紋センサ１６に組み込んでもよい１つの主動作ボタンと、登録モードにおける動作を起動する少なくとも１つの追加ボタンとを含む。ＲＩＳＣプロセッサ２６の主要な機能は、センサ１６が供給する指紋画像を前処理し、強調することである。前処理は、画像の「明瞭化」、背景効果を排除するための画像のクロッピング（ｃｒｏｐｐｉｎｇ）、画像のコントラストの強調、処理容易性が高い２進形態への画像変換を含む。登録モードでは、前処理された画像は、破線４０で示すように、基準画像記憶エリア３２内に格納される。登録は、ユーザが最初にフォブ１４を入手したときに行われ、通常フォブを紛失するか損傷しない限り繰り返さない。セキュリティおよび利便性を高めるために、２つの指紋を登録するようにユーザに問い合わせ、例えば、ユーザが指をけがした場合でも引き続きアクセスできるようにすることが可能である。検証動作モードでは、線４３で示すように、前処理された指紋画像を照合部２８に入力し、線４４を通じて記憶部３２から得た基準画像と比較する。照合部２８は、適切な技法を用いて、所望のセキュリティ・レベルに応じて画像を比較する。処理速度は重要な要素であるので、画像全体のビット毎の比較は通常行わない。代わりに、基準画像の重要な特徴を識別し、新たに走査した画像において同じ特徴を探す。フォブ１４の用途によっては、米国特許第５，０６７，１６２号に開示された技法を、例えば、照合部２８に組み込むとよい。好ましくは、指紋照合部２８は、発明者ブルースW. エバンスその他（Ｂｒｕｃｅ Ｗ. Ｅｖａｎｓ ｅｔ ａｌ.）による「指紋特徴照合装置」（Ｆｉｎｇｅｒｐｒｉｎｔ Ｆｅａｔｕｒｅ Ｃｏｒｒｅｌａｔｏｒ）と題する同時係属中の特許出願の教示に従うとよい。その内容は、この言及により、この明細書にも含まれるものとする。画像比較の結果として、照合部２８は、線４６上に一致信号を発生することができ、これがＣＲＣ発生部３０を活性化する。線４８上に示すように不一致信号が発生した場合、それ以上の処理は行われない。任意選択肢（オプション）として、線４８上の不一致信号を用いて、ユーザ・インターフェース３８上のインディケータを作動させてもよい。

【００２３】線４６上の一致信号によって、巡回冗長符号（ＣＲＣ）発生部３０を作動させると、基準画像データから導出した比較的長い（１２８ビットのような）二進番号を発生する。ＣＲＣは、単一の番号を与え、全ての実用的な目的のために、格納されている基準指紋画像を一義的に識別する。非常に可能性は低いが、２つの指紋画像が同じＣＲＣを生成した場合でも、本発明のシステムの安全性を損なうことはない。これについては以下

で明らかとなろう。

【００２４】ＣＲＣ自体はフォブ１４には格納されず、暗号化された形態でドア受信機１５に送信される。特定のドア１０に初めてアクセスするためにフォブ１４を使用する前に、ユーザ１２は最初にドアに「登録」しなければならない。登録プロセスは、ドアの管理者がユーザ名（口座番号、またはその他の識別情報）を、ユーザのフォブ１４に用いられる公開暗号キーおよびユーザの基準指紋から得られるユーザのＣＲＣと関連付けて格納するプロセスである。例えば、ドア１０が金融機関に対するアクセスを与える場合、ユーザは、登録する際に、彼または彼女のフォブ１４を当該機関に持ち込み、フォブから指紋ＣＲＣをドア受信機１５に送信する。登録モードでは、ドア受信機１５は、ユーザ名またはその他識別情報と関連付けて、ユーザのＣＲＣを格納する。登録プロセスの一部として、ユーザ１２には、フォブ１４以外に何らかの識別を提示することが通常要求され、そのユーザが実際に氏名またはその他の識別情報を提示した人であり、それがドア１０に格納される人であることを金融機関に証明する。

【００２５】自動車のような個人的な色合いが強い所有物に対するアクセスのための登録プロセスは、大幅に単純であるが、この場合もユーザ名または他の識別情報を、ＣＲＣおよびフォブの公開暗号キーと関連付けてドアに格納する。自動車のような個人的所有物でも、例えば、複数の家族メンバーで使用するために、いくつかの異なる個人情報集合を格納する機能を有していなければならない。以下で更に詳細に説明するが、ユーザが登録し終えたドア１０に後にアクセスするためにフォブ１４を使用する場合、フォブはユーザ名および格納されている基準画像に対応するＣＲＣを送信する。すると、ドア１０のロジックが、受信したＣＲＣを、登録の間にユーザ名と共に格納したＣＲＣと比較する。一致が有れば、そのユーザのためにドアが開かれる。

【００２６】図４は、フォブ１４またはその他の個人識別機器とドア１０との間で授受される通信を示し、車のドア１０．１、建物のドア１０．２、自動預金支払機（ＡＴＭ）１０．３、およびコンピュータ１０．４という４つの異なる形態が示されている。各ドア１０はアクチュエータ５０を有し、ドアの開放のような、何らかの所望の動作を行う。また、各ドアはデータベース５２も有し、その中にユーザ名、ユーザのフォブの公開暗号キーおよびユーザのＣＲＣを、ドアを使用するために登録した各ユーザ毎に格納してある。

【００２７】ユーザがフォブ１４を作動させると、線５４で示すように、ユーザ名が暗号化されない状態でドア１０に送信される。任意選択肢として、このステップは、ユーザがドア１０に近づいてくるときに、自動的にトリガするようにしてもよい。線５６で示すように、ドア１０は「起動」コールを送信し、これが近づきつつあるフォブ１４によって受信され、次いでフォブ１４はユーザ名を送信する。

【００２８】ユーザ名を受信すると、ドア１０は、続くメッセージの交換に用いるために、公開暗号キーおよび秘密暗号キーのランダム対を発生する。本発明のこの例示の実施形態では公開キー暗号方式を用いるので、多少の説明は必要であろうが、公開キー暗号方式の原理は安全な通信の分野ではよく理解されていることは認められよう。

【００２９】公開キー暗号方式では、２つの別個の暗号キー、即ち、「公開」キー（誰にでも知られ得るものであり、秘密に保持されていない）および「秘密（プライベート）」キー（一方から他方への通信において、一方にのみ知られている）を用いる。公開キー－秘密キーの対は、これらのいずれかを用いてメッセージを暗号化する場合、その対の他方によってそのメッセージを解読するという特性を有する。例えば、Ａ側が、最初にＢ側の公開キーを用いて暗号化することによって、機密メッセージをＢ側に送ることができる。Ｂのみがこのメッセージを解読することができる。何故なら、解読に必要なＢの秘密キーを有するのはＢだけであるからである。同様に、Ｂは、暗号化にＢの秘密キーを用いて、暗号化メッセージをＡに送ることも可能である。Ａは、Ｂの公開キーを用いてメッセージを解読することができるが、誰でもこれを行うことができる。何故なら、Ｂの公開キーは他の者にも知られているからである。したがって、この公開キー暗号方式の「逆方向」形態（ｂａｃｋｗａｒｄ　ｆｏｒｍ）を用いてメッセージを送信すると、安全ではない場合もある。

【００３０】本発明の図示の実施形態は、公開キー暗号方式の二重暗号形態を用いる。フォブ１４およびドア１０双方が公開キー－秘密キー対を有する。ここで考えられることは、本発明のフォブ１４は「固定」の公開および秘密キー対を有することである。即ち、公開および秘密キーをフォブのユーザ毎に変更しないのである。フォブの公開キーは各ドア１０に登録されており、その使用毎に変更することは実用的でない。フォブの秘密キーはフォブ１４に格納され（図３の３６）、検査やリバース・エンジニアリングによって認識され得ないような形態とすることが好ましい。例えば、通常のどのリバース・エンジニアリング技法でも実際には解読不能であるように、プロセッサ・モジュール２０のシリコン構造内にキーを符号化する。各ドア１０は、当該ドアが新たに使用される毎に、新たな公開－秘密キー対を発生する。このようにすれば、実際のフォブ１４とのメッセージ交換に先立って、これらのキーを判定することはできない。

【００３１】フォブ１４からユーザ名を受信すると、アクセスされようとしているドア１０は、公開－秘密キーのランダム対を発生し、線５８で示すように、暗号化せずにこの公開キーをフォブに送信する。次に、フォブ１

４は、検知した指紋画像と基準画像がうまく一致して、ユーザ識別の有効性を判定した場合、フォブ１４は、発生したＣＲＣに対して、２レベルの暗号化を行う。最初に、フォブ１４内の暗号化ロジック３４は、ドアの公開キーを用いてＣＲＣを暗号化する。次に、得られた暗号化ＣＲＣに対して、フォブの秘密キーを用いて、二重暗号化を行う。二重暗号化ＣＲＣはドア１０に送信され、フォブの公開キーを用い、次いでドアの秘密キーを用いて解読され、ＣＲＣを復元する。次に、ドア１０は、このＣＲＣを、ドアにアクセスしようとしているユーザの名前と関連付けられている、データベース５２内のＣＲＣと比較する。一致があれば、ドア１０はそのアクチュエータ５０にドアを開くように、またはそれ以外の何らかの所望の動作を行うように指令する。

【００３２】この説明から、本発明は保護対象所有物へのアクセスのために非常に安全な技術を提供することが認められよう。フォブ１４は、最初にユーザの指紋が格納されている基準画像と一致しなければ、ドア開放動作を開始することができないように設計されている。フォブを盗んだ者が自身の指紋をフォブ内にうまく再登録したとしても、本当のユーザが登録されている各ドアに格納されているＣＲＣが、泥棒によるドアの動作を防止する。

【００３３】「クローン」フォブを製作しようとしても、フォブの秘密キーを有することができないので、ドアは、クローン・フォブからのメッセージを解読することができないであろう。ある者がフォブの送信を傍受し、その後同じドアを開けようとする試みにおいて、このメッセージをエミュレートしようとした場合、ドアはトランザクション毎に異なる組のキーを用いるために、このたくらみは失敗に終わるであろう。このように、フォブの暗号化メッセージは、いずれのドアに対しても、１回１回異なるものとなる。

【００３４】ドア１０にＣＲＣを最初に暗号化した形態で格納しておくことにより、更にセキュリティ・レベルを強化し、ドアからＣＲＣが盗まれるのを防止することも可能である。

【００３５】以上の説明から、本発明は、防犯機器の分野において、所有物に対するアクセスを制限するための格段の進歩を表すことが理解されよう。即ち、本発明は、単一のハンドヘルド機器を用い、指紋に見られるような、一意の生物測定学的パラメータを用いることによって、その所有者の同一性を非常に信頼性高く検証することにより、人が多くの異なる所有物に対するアクセスを得ることを可能にする。更に、本発明の装置は、リバース・エンジニアリング、「クローン技術」、および保護対象所有物に対するアクセスを得るためのその他の改竄技法に対して高い抵抗力を有する。また、本発明の具体的な実施形態は、例示の目的のために詳細に説明したが、本発明の精神および範囲から逸脱することなく種々の変更も可能であり、特許請求の範囲以外による限定は受けないものとすることは認められよう。

【図面の簡単な説明】

【図１】近くに位置する保護対象所有物へのドアを開くために携帯機器を用いる、本発明の応用を示す図である。

【図２】本発明の主要な構成部品を示すブロック図である。

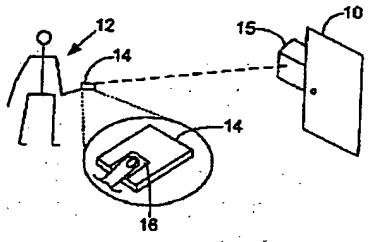
【図３】図２に示すプロセッサ・モジュールの構成部品を示す、更に詳細なブロック図である。

【図４】携帯機器と保護対象所有物へのドアとの間で送信される一連の信号を示すブロック図である。

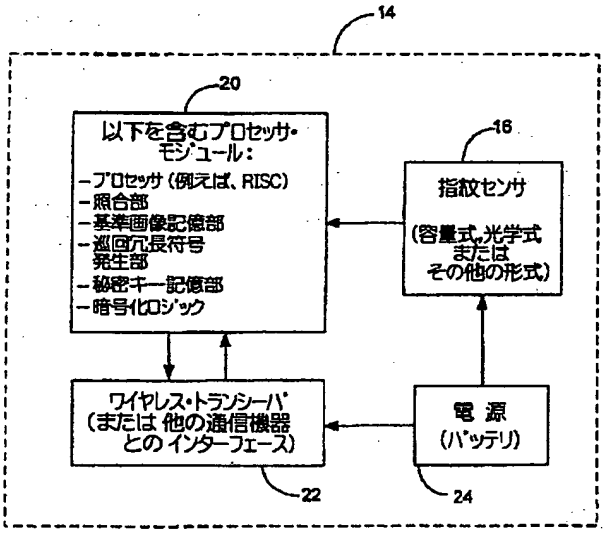
【符号の説明】

１０　ドア
１０．１　車のドア
１０．２　建物のドア
１０．３　自動預金支払機（ＡＴＭ）
１０．４　コンピュータ
１２　ユーザ
１４　小型ハンドヘルド機器（フォブ）
１５　受信機
１６　指紋センサ
２０　プロセッサ・モジュール
２２　トランシーバ
２４　バッテリ電源
２６　プロセッサ
２８　特徴照合部
３０　巡回冗長符号（ＣＲＣ）
３２　基準指紋画像用記憶部
３４　暗号化ロジック
３６　秘密暗号キー用記憶部
３８　ユーザ・インターフェース
５０　アクチュエータ

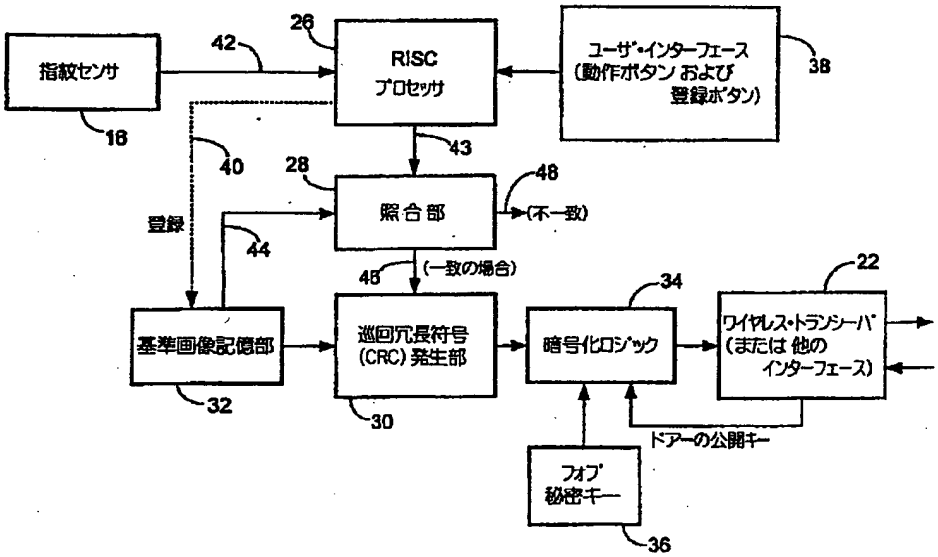
【図１】


12
15
10
14
14
16

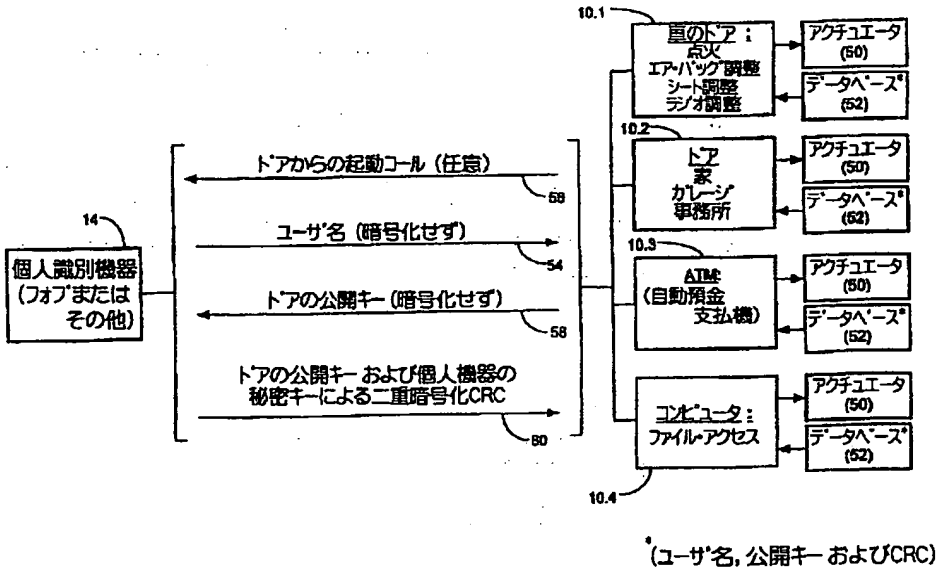
【図２】


14
20
以下を含むプロセッサ・モジュール：
－プロセッサ（例えば、RISC）
－照合部
－基準画像記憶部
－巡回冗長符号発生部
－秘密キー記憶部
－暗号化ロジック
16
指紋センサ
（容量式、光学式またはその他の形式）
ワイヤレス・トランシーバ（または他の通信機器とのインターフェース）
電源（バッテリ）
22
24

【図３】


指紋センサ
16
42
26
RISC プロセッサ
ユーザ・インターフェース（動作ボタンおよび登録ボタン）
38
40
43
28
照合部
48
（不一致）
登録
44
（一致の場合）
46
基準画像記憶部
32
巡回冗長符号（CRC）発生部
30
34
暗号化ロジック
22
ワイヤレス・トランシーバ（または他のインターフェース）
ドアの公開キー
フォブ秘密キー
36

【図４】



【手続補正書】
【提出日】平成１０年１２月２４日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　保護対象所有物に対してアクセスを求める人の同一性を自動的に検証する装置であって、
保護対象所有物に対してアクセスを求める人を識別する生物測定学的データを読み込むセンサと、
前記保護対象所有物に対してアクセスを有することを許可された人を識別する基準生物測定学的データを格納する記憶手段と、
前記格納されている基準生物測定学的データを、前記アクセスしようとする人の生物測定学的データと比較し、これらが一致するか否かについて判定を行う照合部と、
同一性確認をドアに安全に通信し、前記同一性確認の受信時に、前記保護対象所有物に対するアクセスを与える手段と、を備えた装置。
【請求項２】　請求項１記載の装置であって、更に、
検証モードにおいて前記装置の動作を開始する第１のスイッチと、前記装置を登録動作モードに置くように作動する第２のスイッチとを有するユーザ・インターフェースを備え、前記センサからの生物測定学的データを前記記憶手段に格納し、前記検証動作モードにおいて後に検索する、装置。
【請求項３】　請求項１記載の装置において、
前記センサ、前記記憶手段および前記照合部が全て、携帯機器に内蔵されている、装置。
【請求項４】　請求項３記載の装置において、
前記センサ、前記記憶手段および前記照合部が全て、前記人が携行する携帯フォブに内蔵されている、装置。
【請求項５】　請求項３記載の装置において、
前記センサ、前記記憶手段および前記照合部が全て、前記保護対象所有物から離れた通信機器に内蔵されている、装置。
【請求項６】　請求項３記載の装置において、前記安全に同一性確認を通信する手段が、
前記格納されている基準生物測定学的データから数値を発生する手段と、
前記数値を暗号化する暗号化ロジックと、
前記暗号化数値を、前記人に対する識別データと共に前記ドアに送る通信インターフェースと、を含み、前記送信された数値が、登録手続の間に前記人によって予め与えられたものと同じであることを確認した場合、前記ドアが前記保護対象所有物に対する所望のアクセスを与える、装置。
【請求項７】　請求項６記載の装置であって、更に、
前記ドアによって発生されかつ送信された暗号キーを受信する受信機と、
前記携帯機器内に秘密暗号キーを格納する手段と、を備え、前記暗号化ロジックが、前記ドアから受信した前記暗号キーと前記秘密暗号キーとを用いて、前記数値に二重暗号化を施す、装置。
【請求項８】　個人識別フォブであって、保護対象所有

物に対するアクセスのために当該フォブを用いようとするユーザの同一性を自動的に検証し、
保護対象所有物に対してアクセスしようとするユーザを識別する指紋データを読み取るセンサと、
登録手続の間に前記ユーザの基準指紋画像を格納し、今後の使用のために該基準画像を保持するメモリと、
前記格納されている基準画像を、前記アクセスしようとするユーザの前記センサから得られた指紋画像と比較し、２つの画像が一致するか否かについて判定を行う画像照合部と、
同一性確認をドアに安全に通信し、該同一性確認の受信時に、前記保護対象所有物に対するアクセスを与える手段と、を備えたフォブ。

【請求項９】　請求項８記載の個人識別フォブにおいて、前記同一性確認を安全に通信する手段が、
前記格納されている基準指紋画像から数値を発生する手段と、
前記数値を暗号化する暗号化ロジックと、
前記暗号化数値を、前記ユーザ識別データと共に前記ドアに送る送信機と、を含み、前記送信された数値が、登録手続の間に前記ユーザによって予め与えられたものと同じであることを確認した場合、前記ドアが前記保護対象所有物に対する前記所望のアクセスを与える、個人識別フォブ。

【請求項１０】　請求項９記載の個人識別フォブにおいて、
前記数値を発生する手段が、前記格納されている基準指紋画像から巡回冗長符号を発生する手段を含む、個人識別フォブ。

【請求項１１】　請求項９記載の個人識別フォブであって、更に、
前記ドアによって発生されかつ送信された暗号キーを受信する受信機と、
前記フォブ内に秘密暗号キーを格納する手段と、を備え、前記暗号化ロジックが、前記ドアから受信した前記暗号キーと、前記秘密暗号キーとを用いて、前記数値に二重暗号化を施す手段を含む、個人識別フォブ。

【請求項１２】　ドアによって保護されている所有物に対してアクセスしようとするユーザの同一性を自動的に検証する方法であって、
前記ユーザが携行する個人識別機器の一部であるセンサによって、ユーザの生物測定学的データを検知するステップと、
前記検知した生物測定学的データを、前記個人識別機器内に予め格納してある基準生物測定学的データと比較するステップと、
前記検出した生物測定学的データが前記基準生物測定学的データと一致するか否かについて判定を行うステップと、
一致があった場合、前記保護対象所有物に対するアクセスを制御するドアに、同一性確認を安全に伝達するステップと、
前記ドアにおいて前記ユーザの同一性を確認した場合、所望のアクセスを与える機器を作動させるステップと、を含む方法。

【請求項１３】　請求項１２記載の方法であって、更に、
手動スイッチによって、前記個人識別機器の通常動作を開始するステップを含む、方法。

【請求項１４】　請求項１２記載の方法であって、更に、
アクセスしようとするために前記ドアに近づいた場合、該ドアから「起動」メッセージを受信するステップと、
前記「起動」メッセージを受信した場合、前記個人識別装置の通常動作を開始するステップと、を含む、方法。

【請求項１５】　請求項１２記載の方法において、前記安全に通信するステップが、
前記格納されている基準生物測定学的データから数値を発生するステップと、
前記数値を暗号化するステップと、
前記暗号化数値を前記ドアに送信するステップと、
ユーザ識別データを前記ドアに送信するステップと、
前記ドアにおいて、前記暗号化数値を受信しかつ解読するステップと、
前記ドアにおいて登録プロセスの間に前記ユーザによって予め格納されている数値と、前記解読した数値とを比較し、前記ユーザの同一性を確認するステップと、
前記ユーザの同一性が確認された場合、所望の機能を活性化させ、前記保護対象所有物に対するアクセスを与えるステップと、を含む方法。

【請求項１６】　請求項１５記載の方法において、前記安全に通信するステップが、更に、
前記ドアにおいて、ドア公開暗号キーおよびドア秘密暗号キーのランダム対を発生するステップと、
前記ドア公開キーを前記個人識別機器に送信するステップと、
前記機器のそれ以降の使用全てのために、公開および秘密暗号キーの対を、前記個人識別機器に対して選択するステップと、
前記ドア登録プロセスの一部として、前記個人識別機器の公開キーを前記ドアに与えるステップと、
前記個人識別機器の秘密キーを前記機器内に機密的に格納するステップと、を含み、
前記暗号化ステップが、前記ドアの公開キーおよび前記個人識別機器の秘密キーを用いて、前記数値に二重暗号化を施すステップを含む、方法。

【請求項１７】　請求項１６記載の方法において、前記ドアが、
前記個人識別機器の公開キーおよび前記ドアの秘密キーを用いて、前記二重に暗号化された数値を解読する追加

のステップを実行する、方法。

【請求項１８】　正常に施錠されたドアによって保護されている所有物に対するアクセスをユーザが得るための方法であって、

ドアに近づきつつ、フォブ内の指紋センサ上に指を置くステップと、

前記フォブを作動させ、前記ユーザの指紋を検知させかつ記録させるステップと、

前記検知した指紋を、前記フォブ内に予め格納してある基準指紋データと比較するステップと、

比較において合格した場合、前記フォブから、前記所有物を保護する前記ドアに同一性確認を送信するステップと、

同一性確認の受信時に、前記ドアを開錠するステップと、を含む方法。

【請求項１９】　請求項１８記載の方法において、同一性確認を送信する前記ステップが、

前記フォブにおいて前記同一性確認を暗号化するステップと、

前記ドアにおいて前記同一性確認を解読するステップと、を含む、方法。

【請求項２０】　請求項１９記載の方法において、

前記暗号化ステップが、二重暗号化を施すステップを含み、

前記解読ステップが、二重に解読するステップを含む、方法。

【請求項２１】　請求項２０記載の方法において、

前記二重暗号化を施すステップが、最初に、前記ドア内において発生し、該ドアから受信した公開ドア暗号キーを用いて、前記同一性確認を暗号化し、次いで前記フォブ内に格納されている秘密フォブ暗号キーを用いて更に暗号化を行うステップを含み、

前記二重に解読するステップが、最初に、前記ドアにおける以前の登録時に前記ユーザによって与えられた公開フォブ暗号キーを用いて解読を行い、次いで前記ドアにおいて発生した秘密ドア暗号キーを用いて解読を行うステップを含む、方法。

フロントページの続き

(72)発明者　ジェイムズ・エム・リン
アメリカ合衆国ヴァージニア州22066，グレート・フォールズ，ジェイスミス・ストリート　929

(72)発明者　アーサー・エフ・メッセンジャー
アメリカ合衆国カリフォルニア州90278，レドンド・ビーチ，ヴァンダービルト・レーン　2618，アパートメント・ビー

(72)発明者　ブルース・ダブリュー・エヴァンス
アメリカ合衆国カリフォルニア州90277，レドンド・ビーチ，マリーナ・ウェイ　220，ナンバー　3